IN THE MATTER OF THE ROYAL COMMISSION INTO FAMILY VIOLENCE

ATTACHMENT DW-15 TO STATEMENT OF DAVID WATTS

Date of document: 31 July 2015 Filed on behalf of: the Applicant Prepared by: Victorian Government Solicitor's Office Level 33 80 Collins Street Melbourne VIC 3000	[redacted]

This is the attachment marked '**DW-15**' produced and shown to **DAVID WATTS** at the time of signing his Statement on 31 July 2015.

Before me: ..... [redacted]

[redacted]
An Australian legal practitioner
within the meaning of the
Legal Profession Uniform Law (Victoria)

Commissioner
for Privacy and
Data Protection

Privacy Impact Assessment Template

Introduction

The Privacy Impact Assessment Template has been prepared to assist you in conducting a Privacy Impact Assessment (PIA). It is designed to evaluate compliance with the Information Privacy Principles (IPPs) contained in the *Privacy and Data Protection Act 2014* (PDPA), and identify potential privacy risks and risk mitigation strategies. This document should not be considered a substitute for legal advice.

The PIA Template may be used in the preliminary or conceptual phase of a program, in order to identify potential privacy risks or barriers, and then revisited prior to the implementation of a program to ensure that the program complies with privacy obligations.

This PIA assesses information privacy only. Complex initiatives may require an additional assessment of other privacy risks, such as bodily, territorial or locational privacy, and broader privacy considerations required by the *Charter of Human Rights and Responsibilities Act 2006.*

Health information is subject to the *Health Records Act 2001* (HRA). If the proposed program handles any health information, it will need to comply with the Health Privacy Principles (HPPs) in that Act as well. Advice regarding the HPPs should be sought from the Office of the Health Services Commissioner, which regulates the collection and handling of health information in Victoria.

While the IPPs do not specifically apply to health information or de-identified information, this PIA asks you to consider health information as well as any de-identified information that is potentially re-identifiable. A consideration of both these types of information is helpful for a comprehensive information privacy assessment.

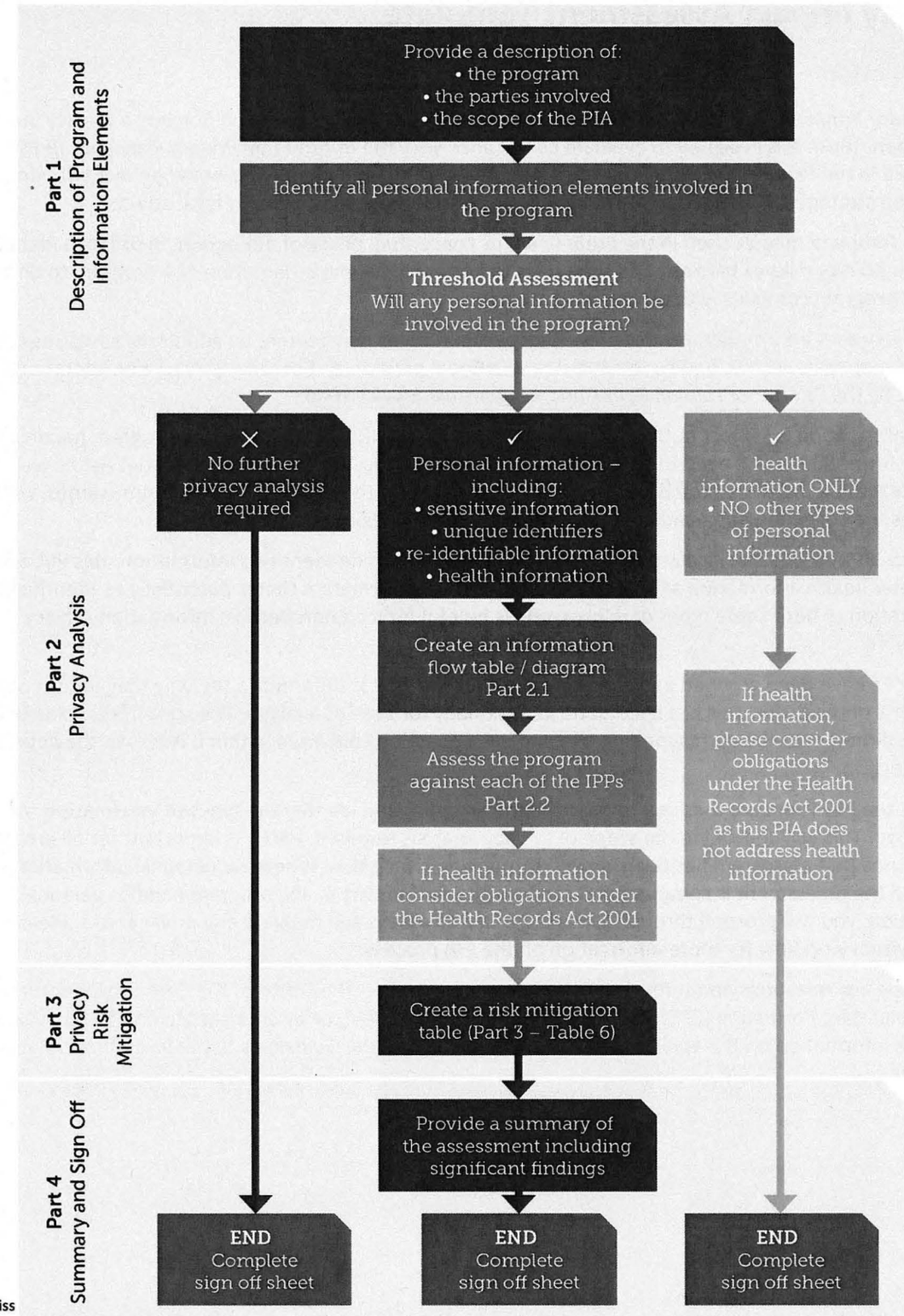
The 10 IPPs have been grouped and considered in an order that is different to the way they are set out in Schedule 1 of the PDPA. This has been done intentionally for ease of analysis. The start of each section provides direction to the corresponding IPP, and each question contained within it refers to the appropriate IPP subsection.

Part 1 of the PIA Template asks you to describe the program and identify the types of information that will be handled. This will determine the scope of privacy analysis required. Part 1 is important for all programs as it ensures that a program has been viewed through a privacy lens. Where no personal information is identified the assessment is complete and can be signed off in Part 4. If a program handles personal information, you will proceed through to Parts 2 and 3 to assess and mitigate any privacy risks. Please see the PIA visual workflow for more information on the PIA process.

If you have any questions about this PIA Template please contact the Office of the Commissioner for Privacy and Data Protection (CPDP) enquiries line on 1300 666 444, or by email at privacy@cpdp.vic.gov.au. For more information on the application of the IPPs please see the *Guidelines to the Information Privacy Principles*.

Commissioner for Privacy and Data Protection

PIA Visual Workflow



Commissioner for Privacy and Data Protection

Privacy Impact Assessment Template

⚠ *This icon identifies where action needs to be taken.*

Part 1 – General Description

Name of Program:

Date:

Name of Department:

PIA Drafter:

Email: Phone:

Program Manager:

Email: Phone:

Are you a law enforcement agency as defined in Section 3 of the PDPA? Y/N

ⓘ **Definition – Program**
For the purpose of this document, program will be used to mean any system, legislation, project, initiative or activity.

⚠ *For questions in the following section, delete the italicised descriptive text and replace it with your own.*

1. Description of the Program and Parties

This section should provide a description of the program and the context in which it functions, including: the purpose of the program and how it functions, its expected benefits, any other process or program (if any) of which it is a part, the legal authority the organisation has to implement the program, all other parties involved and the roles they play, including a description of all contracted service providers (CSPs) etc.*

**The privacy protections required under the PDPA are carried forward to any CSP but only in relation to the CSPs provision of service under a state contract. An example of a CSP would be a non-profit organisation that receives funding to deliver government welfare services to the public. Please refer to the Outsourcing and Privacy Guidelines for additional information on CSPs.*

2. Scope of this PIA and any Related Privacy Impact Assessments

This section should explain, where applicable, exactly what part or phase of the program the PIA covers and, where necessary for clarity, what it does not cover. This section should also identify, where applicable, any PIAs for other parts of the program that have already been completed or that will be undertaken at a later date. Please also identify if you have any public interest determinations, information usage arrangements or certifications in place under the PDPA related to this program.

3. Identifying Information Elements

This section considers the use of information that is capable of identifying an individual, whether directly or indirectly. This includes any information that is collected, used or disclosed by a CSP on behalf of your organisation for the purpose of this program.

3.1 Personal Information

When assessing impacts to privacy the first consideration is whether any personal information will be involved in the program. Section 3 of the PDPA defines personal information as follows:

Commissioner for Privacy and Data Protection

> **Definition – Personal Information**
> Personal information means information or an opinion (including information or an opinion forming part of a database), that is recorded in any form and whether true or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion, but does not include information of a kind to which the Health Records Act 2001 applies.

Please list or attach as an appendix, all the personal information the program will collect, use or disclose.

3.2 Sensitive Information

The PDPA contains specific provisions relating to the collection of sensitive information (IPP 10). While there are many types of information that attract a heightened duty of care, for example banking details, the IPPs that specifically apply to sensitive personal information in the PDPA only apply to those in the table below.

Table 1: Sensitive Information

Please check all the types of sensitive information your program will collect, use or disclose.

a	Racial or ethnic origin
b	Political opinions
c	Membership of a political association
d	Religious beliefs or affiliations
e	Philosophical beliefs
f	Membership of a professional or trade association
g	Membership of a trade union
h	Sexual preferences or practices
i	Criminal record

This program will not collect, use or disclose any of the above information

3.3 Unique Identifiers

The PDPA has specific requirements for the collection, use and disclosure of unique identifiers (IPP 7). The PDPA defines a unique identifier as follows:

> **Definition – Unique Identifier**
> Unique identifier means an identifier (usually a number) assigned by an organisation to an individual to uniquely identify that individual for the purposes of the operations of the organisation but does not include an identifier that consists only of the individual's name, but does not include an identifier within the meaning of the Health Records Act 2001.

An example of a unique identifier is a tax file number, a driver's license number, a passport number or a Centrelink Customer Reference Number.

Commissioner for Privacy and Data Protection

Table 2: Unique Identifiers

Please complete Table 2.

1	Will this program assign a unique identifier? Y/N

If YES, please explain how the unique identifier is necessary for the program:

2	Will this program collect, use or disclose a unique identifier created by another organisation? Y/N

If YES, please describe the unique identifier, specify the organisation from which the identifier came, and the reason the identifier is necessary for your organisation to carry out its functions:

3.4 Health Information

While the PDPA does not apply to health information, the privacy protections that should be considered are comparable to those necessary for personal information under the PDPA. This is demonstrated by the similarity between the IPPs and the HPPs contained in the HRA.

Definition – Health Information

The HRA defines health information as:

a) information or an opinion about-
   (i) the physical, mental or psychological health (at any time) of an individual; or
   (ii) a disability (at any time) of an individual; or
   (iii) an individual's expressed wishes about the future provision of health services to him or her; or
   (iv) a health service provided, or to be provided to an individual – that is also personal information; or

b) other personal information collected to provide, or in providing, a health service; or

c) other personal information about an individual collected in connection with the donation, or intended donation, by the individual of his or her body parts, organs or body substances; or

d) other personal information that is genetic information about an individual in a form which is or could be predictive of the health (at any time) of the individual or of any of his or her descendants – but does not include health information, or a class of health information or health information contained in a class of documents, that is prescribed as exempt health information for the purposes of this Act generally or for the purposes of specified provisions of this Act.

Table 3: Health Information

Please complete Table 3.

1	Will this program collect, use or disclose health information? Y/N

If YES, please describe the health information.

3.5 Re-identifiable Information

Commissioner for Privacy and Data Protection

Many programs rely on the use of de-identified or non-identifiable information. When such information is used it needs to be treated with caution and afforded many of the same privacy protections as personal information, where there is the potential for re-identification to occur. This is particularly the case where a program involves data matching/linking activities. For that reason, when assessing privacy of personal information, potentially re-identifiable information should be protected in the same way as personal information.

The National Health and Medical Research Council of Australia provides the following definitions, which should assist in determining when information should be considered re-identifiable (https://www.nhmrc.gov.au/book/glossary).

> **Definition – Re-identifiable Data**
> Re-identifiable data is data from which identifiers have been removed and replaced by a code, but it remains possible to re-identify a specific individual by, for example, using the code or linking different data sets.

> **Definition – Non-identifiable Data**
> Non-identifiable data is data that has never been labelled with individual identifiers or from which identifiers have been permanently removed, and by means of which no specific individual can be identified. Subsets of non-identifiable data are those that can be linked with other data so it can be known they are about the same data subject, although the person's identity remains unknown.

Table 4: Re-identifiable Information

Please complete Table 4.

1	Will this program collect, use or disclose re-identifiable information? Y/N

If YES, please describe the process of de-identification and potential for re-identification.

Table 5: Threshold Assessment:

Please complete Table 5.

Based on the information above, does your program collect, use or disclose:		Y	N
1	Personal information (which may include any of sensitive information, unique identifiers, re-identifiable information or health information)? *If YES, please proceed with the rest of the assessment. If NO, continue to sign off page.*		
2	Health information ONLY (and no other types of personal information)? *If YES, please proceed to sign off page and consider your obligations under the HRA. Please contact the Health Services Commissioner for further assistance. If NO, continue to question 3.*		

> **Definition – De-identified**
> The PDPA defines the term de-identified, in relation to personal information as meaning that the information no longer relates to an identifiable individual or an individual who can be reasonably identified.

Commissioner for Privacy and Data Protection

3	Personal information (including sensitive information, unique identifiers, re-identifiable information) AND health information? *If YES, please proceed with the rest of this assessment and consider your obligations under the HRA. Please contact the Health Services Commissioner for further assistance.*	

Part 2 – Privacy Analysis

2.1 Information Flow Table/Diagram

Please be as detailed as possible in describing the elements of personal information involved. This can be done as a flow table or diagram. Please include:

* *Each element of personal information, including sensitive information, unique identifiers, health information and re-identifiable information*
* *How each element will be collected, used and disclosed, and by whom*
* *Any transfer of personal information to someone outside of Victoria (other than the organisation or the individual the information is about).*

If multiple organisations will collect, use or disclose personal information, the diagram or table should identify how each organisation is involved in the program.

This table/diagram will be used to inform the assessment of the program against the IPPs in section 2.2.

2.2 Information Privacy Principles

These questions relate to the personal information described in Part 1 and set out in the flow table/ diagram in section 2.1. This section will assist you in assessing your program against each of the IPPs and determining which are applicable. Each question below has a corresponding IPP. Detailed information about each IPP can be found in the Guidelines to the Information Privacy Principles, and may assist you in answering each question. The orange row at the end of each section will assist you to identify where you may have a privacy risk. Where a risk is identified this should be noted in Part 3 – Privacy Risk Mitigation.

Collection of Personal Information (including sensitive information and unique identifiers)
(Refer to IPPs 1, 7, 8 & 10)

Collection		Y	N	IPP
1	Is all the information collected NECESSARY for the program?			1.1
2	Is it lawful or practicable for the individual to remain anonymous for the purpose of the program?			8.1
Risk Identifier: If the answer to question 1 is NO, please address Collection as a risk in Part 3 – Privacy Risk Mitigation. If the answer to question 2 is YES and the program will collect personal information, please address Anonymity as a risk in Part 3 – Privacy Risk Mitigation.				
Notice				
3(a)	Have you taken reasonable steps to ensure that the individual whose information is collected is made aware of the information below? *If YES, please describe how:*			1.3

Commissioner for Privacy and Data Protection

The identity of the organisation and how to contact it
The fact that the individual can access their information
The purpose for the collection
To whom the organisation will disclose the information
Any law requiring the information to be collected
Consequences, if any, to the individual if the information is not provided

3(b)	If the answer to question 3(a) is NO, is the collection done by a law enforcement agency for a law enforcement function or activity? (For further information see Section 15 of the PDPA).			

Risk Identifier: If the answers to questions 3(a) and (b) are both NO please address Notice as a risk in Part 3 – Privacy Risk Mitigation.

Direct/Indirect Collection

4(a)	Is the information being collected DIRECTLY from the individual?	1.4
4(b)	*If the answer to question 4 is NO, please check the exception to the notice requirement that applies.*	
	Reasonable steps have been taken to ensure the individual whom the information is about has been made aware of the information in question 3; OR	1.5
	It would pose a serious threat to the life or health of any individual if the matters in question 3 were communicated to the individual	

	The collection is by a law enforcement agency for a law enforcement function or activity (for further information see Section 15 of the PDPA).			

Risk Identifier: If the answers to questions 4(a) and (b) are all NO, please address Indirect Collection as a risk in Part 3 – Privacy Risk Mitigation.

Unique Identifier
(Please answer question 5 if your program will assign or collect a unique identifier, as identified in Table 2)

5(a)	Will this program assign or collect a unique identifier (see Table 2 above). *If NO, proceed to question 6.*	
5(b)	Is it NECESSARY to assign a unique identifier to enable your organisation to carry out its program?	7.1
5(c)	Will a unique identifier <u>of another organisation</u> be used ONLY if one of the following conditions is met?	7.2
	It is necessary for your organisation to carry out its functions (this should be described in Table 2 above); OR	
	The individual has consented to the use; OR	
	It is an outsourcing organisation adopting the unique identifier of a CSP performing obligations under a state contract	
5(d)	An individual will not be required to provide a unique identifier unless authorised by law or in connection with the purpose for which the unique identifier was originally assigned. *If YES, please explain:*	7.4

Risk Identifier: If the answers to questions 5(b)-(d) are all NO, please address Unique Identifiers as a risk in Part 3 – Privacy Risk Mitigation.

Commissioner for Privacy and Data Protection

Sensitive Information (Please answer question 6 if your program will collect sensitive information, as identified in Table 1)		
6(a)	Will this program collect sensitive information (see Table 1 above). *If NO, proceed to question 8.*	
6(b)	Sensitive information identified in Table 1 will not be collected unless one of the following apply:	10.1
	The individual has consented	10.1(a)
	The collection is required under law	10.1(b)
	The collection is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual, where the individual that the information is about is physically or legally incapable of consenting or physically cannot communicate the consent	10.1(c)
	The collection is necessary for the defence of a legal or equitable claim	10.1(d)
Risk Identification: If the answer to question 6(b) is NO please address Sensitive Information as a risk in Part 3 – Privacy Risk Mitigation.		
7(a)	Will the sensitive information be used for a research purpose? *If NO, proceed to question 8.*	
7(b)	If sensitive information is used for research purposes all of the following conditions must be met:	
	The collection is necessary for research, compilation or analysis of statistics for a government funded welfare or educational service or if relating to racial or ethnic origin, the information is collected for providing government funded welfare or educational services; AND There is no reasonably practicable alternative to collecting the sensitive information for that purpose; AND It is impracticable for the individual to consent.	10.2(a)(i) 10.2(a)(ii) 10.2(b) 10.2(c)
Risk Identification: If the answer to question 7(b) is NO, please address Sensitive Information as a risk in Part 3 – Privacy Risk Mitigation.		

Use and Disclosure of Personal Information (including unique identifiers) *(Refer to IPPs 2 & 7)*

Use and Disclosure		Y	N	IPP
8	Information will ONLY be used or disclosed for the primary purpose identified in Part 1. *If YES, proceed to question 10.*			2.1
9(a)	In addition to using and disclosing information for the primary purpose it was collected, personal information will be used or disclosed for a secondary purpose. *If YES, please check which of the following secondary purposes below apply (9(b)-9(j)):*			
9(b)	a) The secondary purpose is related to the primary purpose, or for sensitive information, directly related to the primary purpose; AND			2.1(a)

Commissioner for Privacy and Data Protection

	b) the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose *If YES, please describe the secondary purpose:*			
9(c)	The individual has consented (express or implied) to the use or disclosure			2.1(b)
9(d)	As necessary for research, or the compilation or analysis of statistics IN THE PUBLIC INTEREST			2.1(c)
9(e)	Where necessary to lessen or prevent a serious and imminent threat to an individual's life, health, safety or welfare; or a serious threat to public health, public safety or public welfare			2.1(d)
9(f)	Where necessary on suspicion or unlawful activity as part of its investigation or reporting its concerns to relevant persons or authorities			2.1(e)
9(g)	As required or authorised by law *If YES, please site the relevant law:*			2.1(f)
9(h)	By or on behalf of a law enforcement agency for one of the following purposes: (* a written note must be made of any use or disclosure made under this section) (i) the prevention, detection, investigation, prosecution or punishment of criminal offences or breaches of a law imposing a penalty or sanction (ii) the enforcement of laws relating to the confiscation of the proceeds of crime (iii) the protection of the public revenue (iv) the prevention, detection, investigation or remedying of seriously improper conduct (v) the preparation or conduct of proceedings or implementation of the orders of any court or tribunal			2.1(g)/ 2.2
9(i)	As requested, in writing by the Australian Security Intelligence Organisation (ASIO) or the Australian Secret Intelligence Service (ASIS)			2.1(h)
9(j)	The use or disclosure is by a law enforcement agency for a law enforcement function or activity (for further information see Section 15 of the PDPA)			
Risk identification: If the answer to question 9(a) is YES and 9(b)-(j) are all NO please address Secondary Purpose as a risk in Part 3 – Privacy Risk Mitigation.				
Use and Disclosure of a Unique Identifier (assigned by another organisation)		Y	N	IPP
10(a)	This program will use or disclose a unique identifier assigned to an individual by another organisation (see Table 2 above). *If NO, proceed to question 11.*			7.2
10(b)	The unique identifier assigned to an individual by another organisation will not be used or disclosed unless one of the following apply:			7.3
10(c)	It is necessary for the organisation to fulfil its obligation to the other organisation			7.3(a)
10(d)	The individual has consented			7.3(c)
10(e)	One or more of the following apply: (see IPP 2.1(d)-(g) for full conditions)			7.3(b)
10(f)	A serious threat to individual or public health, safety or welfare			

Commissioner for Privacy and Data Protection

10(g)	Reporting a suspected unlawful activity to the relevant person or authority as part of an investigation
10(h)	It is required or authorised by law *If YES, please site the relevant law:*
10(i)	The organisation reasonably believes the use or disclosure is reasonably necessary by or on behalf of a law enforcement agency (see IPP 2.1(g) for full description)

Risk Identifier: If the answer to question 10(a) is YES and 10(c)-(i) are all NO please address Secondary Purpose as a risk in Part 3 – Privacy Risk Mitigation.

Commissioner for Privacy and Data Protection

***Transborder Data Flows** (Refer to IPP 9)*

Transborder Data Flows		Y	N	IPP
11(a)	The program will transfer personal information to an organisation or person outside of Victoria (other than the organisation or the individual). *If NO, proceed to question 12. If YES, please describe:*			
11(b)	Personal information will only be transferred to someone outside of Victoria (other than the organisation or the individual) if one of the following (11(c)-11(h)) apply:			9.1
11(c)	The organisation reasonably believes that the recipient is subject to laws or a contract enforcing information handling principles substantially similar to the IPPs			9.1(a)
11(d)	The individual consents to the transfer			9.1(b)
11(e)	The transfer is necessary for the performance of a contract between the individual and the organisation			9.1(c)
11(f)	The transfer is necessary as part of a contract in the interest of the individual between the organisation and a third party			9.1(d)
11(g)	All of the following apply: The transfer is for the benefit of the individual; AND It is impractical to obtain consent; AND If it were practicable the individual would likely consent.			9.1(e)
11(h)	The organisation has taken reasonable steps so that the information transferred will be held, used and disclosed consistently with the IPPs *If YES, please describe steps:*			9.1(f)

Risk Identification: If the answer to question 11(a) is YES and 11(c)-(h) are all NO please address Transborder Data Flows as a risk in Part 3 – Privacy Risk Mitigation.

***Data Quality** (Refer to IPP 3)*

Data Quality	IPP 3.1
13. Please describe steps taken to ensure that all data that is collected, used or disclosed will be accurate, complete and up to date. *For example, check to see that the information was obtained from a reputable source such as another government agency, ensure the system is regularly tested for accuracy, conduct periodic reviews of the information, a retention schedule in place that deletes information that is over a year old, staff are trained in the use of the tools and receive periodic updates, reviews of audit trails are undertaken regularly, independent oversight, incidents are reviewed for lessons learnt and systems / processes updated appropriately*	

Risk Identification: If the program does not ensure that all data collected, used or disclosed is accurate, complete and up to date, please address Data Quality as a risk in Part 3 – Privacy Risk Mitigation.

Commissioner for Privacy and Data Protection

Security of Personal Information *(Refer to IPP 4)*

IPP 4 requires an organisation to take reasonable steps to protect the personal information it holds from misuse, loss and from unauthorised access, modification and disclosure. Once developed and approved, the Victorian Protective Data Security Framework (VPDSF) will provide implementation guidance on data security for the Victorian public sector. For this program please ensure you have considered the requirements of the Australian government's Protected Security Policy Framework as adapted to Victoria until the VPDSF is issued.

Data Security		Y	N	IPP
12(a)	The program has taken reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure. *Please describe steps. For example, the program should have data protection governance arrangements in place covering all the security domains including: Security policies and procedures, security risk management, information access, security training and awareness, security incident management, business continuity management, third party management (CSPs/government services), information security, information sharing, personnel security, ICT security, physical security.*			4.1 & VPDSF
Risk Identification: If the program does not address the security risks identified in 12(a) please address Data Security as a risk in Part 3 – Privacy Risk Mitigation.				
Records Management		**Y**	**N**	**IPP**
12(b)	The program will take reasonable steps to destroy or de-identify personal information if it is no longer needed for any purpose. *If YES, please list the steps or the relevant records Retention and Destruction Authority (RDA) under the Public Records Act 1973.*			4.2
Risk Identification: If the answer to question 12(b) is NO, please address Records Management as a risk in Part 3 – Privacy Risk Mitigation.				

Openness *(Refer to IPP 5)*

Openness		Y	N	IPP
14(a)	The organisation has a document available for public review that sets out the policies for the management of personal information. *Please identify document(s) and provide link where available:*			5.1
14(b)	The organisation has steps in place to allow an individual to know what personal information it holds about them and for what purposes it collects, uses and discloses it.			5.2
Risk Identification: If the answer to question 14(a) or (b) is NO, please address Openness as a risk in Part 3 – Privacy Risk Mitigation.				

Access and Correction *(Refer to IPP 6)*

The Access and Correction principle (IPP 6) entitles individuals to view and obtain copies of their personal information and to correct personal information held about them. IPP 6 is designed to supplement existing access and correction rights under the *Freedom of Information Act 1982* (FOI Act). Information held by a Victorian public sector organisation is subject to the FOI Act and therefore do not need to assess against IPP 6.

Commissioner
for Privacy and
Data Protection

Where the public sector outsources part of their program services to a CSP, the CSP will be required to comply with IPP 6 but only in relation to the CSP's provision of service under a state contract. Please refer to Outsourcing and Privacy Guidelines for additional information on CSPs and their obligations under IPP 6.

Commissioner for Privacy and Data Protection

Part 3 – Privacy Risk Mitigation

Table 6: Risk Mitigation

For the purpose of this section, a risk is something that could lead to the unauthorised collection, use, disclosure or access to personal information.

There are a number of other risks that could arise that do not relate directly to the IPPs. For example, the risk that personal information might be produced where non-identifiable data are subject to data matching/linking or data analytics. Further, community expectations of how public sector organisations should use personal information are important to consider. Even where an act or practice does not contravene the IPPs, individuals may be uncomfortable with the use of their information for particular purposes. Please consider an assessment of all risks related to personal privacy.

It is important to note that while identifying and mitigating privacy risks is a critical component of good privacy practice, risk mitigation does not provide an alternative to compliance with the IPPs. Privacy needs to be incorporated with other program goals, such as security or functionality and not balanced against them. A public sector agency must ensure that any handling of personal information is aligned with privacy legislation and only departs from the requirements in very limited circumstances. See the *Public Interest Determinations* discussion below for acceptable departures from the IPPs.

⚠ *Please list each of the privacy risks identified by the checklist and the mitigation strategies/tools that will be implemented to mitigate these. Add extra rows as required. If you have concerns as to how an identified risk can be addressed please contact CPDP to discuss strategies. Please specify the likelihood of the risk arising, the degree of impact it would have on individuals' privacy if it occurred, and an assessment (low, medium or high) of the residual risk.*

Risk Mitigation Table					
	Identified Risk	Mitigation Strategy	Likelihood	Impact	Risk Rating
1					
2					
3					
4					

New Risk Mitigation Option: Public Interest Determinations

The PDPA requires organisations to comply with each of the IPPs. However, where there is a public interest in an organisation not complying with one or more of the IPPs (with the exception of IPP 4 – Data Security and IPP 6 - Access and Correction), they may apply for a public interest determination (PID). If your organisation is not compliant with one or more of the IPPs for this program, as identified by the above checklist, a PID may be appropriate if there is an overriding public interest in non-compliance. For a full discussion of PIDs, see the *Guidelines to Public Interest Determinations, Temporary Public Interest Determinations, Information Usage Arrangements and Certification*.

Commissioner
for Privacy and
Data Protection

Commissioner
for Privacy and
Data Protection

Part 4 – Summary of Assessment and Sign Off

Summary

⚠ *Insert a summary or overview of the most significant findings in relation to both identified privacy risks and identified privacy-enhancing features. Where appropriate also include critical recommendations. The summary should include an overview of which privacy risks cannot be mitigated, the likely public reaction to such risks, and whether the risks are outweighed by the public benefit in the project proceeding.*

Signatures

Program/Department Manager	Signature	Date
Head of Public Body, or delegate	Signature	Date